【重要なお知らせ】ランサムウェアによる不正アクセスに関するご報告（第四報）

2026 年 2 月 13 日
株式会社東北新社　代表取締役社長　小坂恵一
株式会社オムニバス・ジャパン　代表取締役社長　丸井庸男

平素は格別のご高配を賜り、厚く御礼申し上げます。

2025 年 12 月 9 日に発覚いたしました、株式会社オムニバス・ジャパン（以下「オムニバス・ジャパン」といいます。）に対するランサムウェア攻撃による不正アクセス事案（以下「本件」といいます。）に関し、外部専門機関より、フォレンジック調査結果に関する暫定的な報告（以下「フォレンジック調査」といいます。）を受領いたしましたので、同報告に基づき、現時点で判明している内容をご報告申し上げます。

なお、2025 年 12 月 17 日付けの第一報、同月 26 日付けの第二報、および 2026 年 1 月 22 日付けの第三報の内容はこちらです。

１．本件の概要

外部の攻撃者（以下「攻撃者」といいます。）からのサイバー攻撃により、オムニバス・ジャパンが運用するサーバーにおいて不正アクセス事案が発生したことが 2025 年 12 月 9 日に発覚いたしました。また、攻撃者によって、オムニバス・ジャパンが運用するサーバーに保管されていた一部の情報の暗号化と持ち出しがなされ、さらに、当該情報の一部がダークウェブ上のリークサイトに公開される事象を確認いたしました。

フォレンジック調査の結果、計 11 台のサーバー（以下「本件不正アクセスサーバー」といいます。）への不正アクセス、本件不正アクセスサーバーおよび他 1 台のサーバー（以下、総称して「本件感染サーバー」といいます。）内のファイルの暗号化、ならびに本件感染サーバーのうち 1 台に保存されていたファイルの外部送信の痕跡が確認されております。また、本件感染サーバーのうち 1 台に保存されていたファイルと同一のファイルが、ダークウェブ上のリークサイトに公開されていることを確認しております。

弊社およびオムニバス・ジャパンではさらなる詳細調査を実施しております。また、リークサイトに掲載された情報につきましては、引き続き、掲載情報の精査を進めると共に、更なる情報掲載等がないかを継続監視しております。

なお、現時点で、ダークウェブ上のリークサイト以外での情報公開や、SNS 等を通じた情報の拡散、本件に起因するお客様の個人情報を用いた不正利用等の二次被害については、確認されておりません。

２．現時点で判明している事実に基づき推定される原因

今回のフォレンジック調査では、本件発生の原因の完全な究明には至りませんでしたの

で、弊社およびオムニバス・ジャパンでは、外部専門機関の協力のもと、さらなる詳細調査を実施しております。現時点で判明している事実に基づくと、本件の原因は、アカウント管理や不審挙動監視の課題等をついて、攻撃者が、サーバーの管理者アカウントの ID およびパスワードを何らかの形で不正に取得し、オムニバス・ジャパンのサーバー内にアクセスしたことにあると推定されます。

３．現在の復旧状況と見通し

弊社およびオムニバス・ジャパンでは、インターネット接続点の管理を強化するために、セキュリティを強化した新しいネットワークセグメントの構築を進めております。

業務の再開にあたり、外部専門機関の監修のもと、安全性が担保された新環境への移行を徹底しております。具体的には、移行対象となるすべてのデータに対して厳格なスクリーニングを実施し、一切の脅威が含まれていないことを確認した上で、新しいインフラへ集約・配置する対応を進めております。

現時点では、2026 年春頃を目処に、新しいセキュアなインフラへの完全移行と、本格的な業務復旧を完了させる計画です。

オムニバス・ジャパンのシステムおよびサービスの完全な復旧には、引き続き時間を要する見込みです。現在、お客様からご依頼いただいている納品物につきましては、出来る限りの対応をさせて頂いています。

４．再発防止策

オムニバス・ジャパンは、事案発覚後直ちに、本件感染サーバーのオムニバス・ジャパンのネットワークからの遮断および、ルーターの不審な設定の削除を完了いたしました。また、不正な活動の再発を防止するため、高度なエンドポイント検知・対応ソリューション（EDR）を導入し、24 時間体制での監視を実施しております。

弊社およびオムニバス・ジャパンでは、単なるデータの復元にとどまらず、根本から安全な IT 基盤を再構築するため、現在、フォレンジック調査を担当した外部専門機関と連携して、アクセス制限強化やセキュリティ規定見直し等の対策について段階的な実施、導入の検討および協議を進めております。

５．今後の見通し

引き続き、関係各所および外部専門機関と連携して、早期の全面復旧および本件の全容解明、ならびに、実効性の高い再発防止策の策定に向けて全力で取り組んでまいります。

皆様には、多大なるご心配をおかけいたしますことを深くお詫び申し上げます。

＜本件に関するお問い合わせ先＞

株式会社東北新社
toiawase_security@tfc.co.jp

（これまでの対応経緯の詳細）

本件に関する現時点での弊社およびオムニバス・ジャパンの対応経緯は、以下のとおりです。

- 2025 年 12 月 9 日：オムニバス・ジャパンの使用するシステムの一部が、ランサムウェアを用いたサイバー攻撃の被害を受け、当該システム内の一部のファイルが暗号化され、アクセスできない状態となっていることを確認し、外部専門機関に調査を依頼。その後、オムニバス・ジャパンおよび弊社合同の対策本部を設置。
- 12 月 11 日：警察署へ被害相談の実施。
- 12 月 12 日：独立行政法人情報処理推進機構（IPA）へ報告。
- 12 月 17 日：これまでの調査状況を踏まえ、個人情報保護委員会へ速報を提出。また、弊社およびオムニバス・ジャパンのホームページにおいて、第一報を公表。
- 12 月 24 日：攻撃者のリークサイトにおいてオムニバス・ジャパンの社名が掲載され、一部のお取引先様の情報が公開されたことを確認。
- 12 月 26 日：弊社およびオムニバス・ジャパンのホームページにおいて、第二報を公表。
- 2026 年 1 月 22 日：弊社およびオムニバス・ジャパンのホームページにおいて、第三報を公表。